

Quantum Synchronizable Codes From Augmentation of Cyclic Codes

Yixuan Xie and Jinhong Yuan

School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia
Email: Yixuan.Xie@student.unsw.edu.au, J.Yuan@unsw.edu.au

Abstract—We propose a new method to construct quantum synchronizable codes from classical cyclic codes using the idea of augmented cyclic codes. The method augments a dual-containing cyclic code \mathcal{C}_2 to obtain another cyclic codes \mathcal{C}_1 of higher dimension. The resulting two cyclic codes and the dual code \mathcal{C}_2^\perp satisfy the containing property $\mathcal{C}_2^\perp \subset \mathcal{C}_2 \subset \mathcal{C}_1$. The proposed construction method based on general quadratic residue sets of size $p = 2^{l+2} - 1$, such that the constructed quantum synchronizable codes are Calderbank-Shor-Steane (CSS) quantum error correcting codes. We show that the proposed construction method yield $(c_l, c_r) - \lceil [p + c_l + c_r, 1] \rceil$ quantum synchronizable codes that can tolerate maximum number of misalignment errors.

I. INTRODUCTION

In the past decades, quantum information theory has experienced remarkable progress towards developing and realizing large scale quantum computation and quantum communication. Since the theory of quantum error-correcting codes discovered in [1], researchers have dealt with the effects of decoherence on quantum states by regarding noise errors as linear combinations of operators that act on qubits [2][3]. The simplest error model of this kind is the *Pauli operators* I, X, Y, Z . This error model may be considered as quantum version of additive noise, which is the most important and well-studied error model. The theory of quantum error-correction and the concepts of design quantum error-correcting codes to correct such errors were also well studied in the literature [4]-[12].

Moreover, *misalignment* with respect to the frame size of a data stream is a type of *synchronization errors* that do not fall into the category of additive noise. To describe a misalignment error, assuming frame synchronization was established at the beginning of transmission to a noisy quantum channel. However, frame synchronization may be lost during quantum communications or quantum computations. This type of error occurs when the boundary of each block of data locates incorrectly by a certain number of positions towards the left or right. Then error correction procedures performed based on the wrongly positioned blocks may generate errors that the original fully aligned block might not experience on any qubits within the block.

To be able to correct these errors (block misalignment and additive noise), the theoretical framework on *quantum synchronizable code* was investigated in [13]-[15]. A quantum synchronizable code is a coding scheme that encodes a number of logical qubits into a certain number of physical qubits and

it can correct misalignment by up to c_l qubits to the left and up to c_r qubits to the right when block synchronization is lost during transmission. The standard error correction procedure using a quantum error correcting code can also be performed to correct any additive errors occurred prior to the procedure of synchronization recovery. The authors in [13]-[15] showed that ‘cyclic’ property of a linear code is the key to perform synchronization recovery, and they developed narrow-sense BCH codes and punctured Reed-Muller codes as two classes of quantum synchronizable codes. Moreover, the authors also handled bit and phase errors caused by Pauli X and Z operators in two separate steps by employing the Calderbank-Shor-Steane (CSS) quantum error correcting codes [4][5].

In this work, we propose a new method to construct quantum synchronizable codes by exploiting some peculiar properties of classical cyclic codes over the finite field \mathbb{F}_2 . We then show that by adopting quadratic residue sets into the proposed method to construct quantum synchronizable codes, the tolerance of misalignment errors meets the upper bound under certain condition. In Section II, we review some preliminary results of classical cyclic codes. Section III introduces the concept of quantum synchronizable codes and the procedure of synchronization recovery. We then discuss the proposed method of the construction of a quantum synchronizable code based on quadratic residue sets in Section IV. Finally, Section V concludes the paper with possible future works.

II. PRELIMINARIES

In this paper, we consider only the binary (\mathbb{F}_2) cyclic codes of length n . As usual, we define a binary linear code $[n, k]$ as a k -dimensional subspace of the n -dimensional vector space \mathbb{F}_2^n , whereas a quantum code that encodes k -qubits into n -qubits is defined as $[[n, k]]$. We denote the lowest common multiple and the greatest common divisor of a polynomial as $\text{lcm}(\cdot)$ and $\text{gcd}(x)$, respectively. We also denote the degree of a polynomial as $\text{deg}(\cdot)$ and the dimension of a code as $\text{dim}(\cdot)$.

1) *Cyclic Codes and Dual Codes*: A Cyclic code \mathcal{C} is a linear $[n, k]$ code if $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$ is a codeword of \mathcal{C} , then every cyclic shift of \mathbf{c} , denoted by $\pi_s(\mathbf{c})$, is also a codeword of \mathcal{C} . Let $k = \text{dim}(\mathcal{C})$, then $r = n - k$ be the number of redundancy of the cyclic code. It is also known that a cyclic code can be seen as a principal *ideal* in the ring $\mathbb{F}_2[x]/(x^n - 1)$ that is generated by the unique monic

polynomial $g(x)$ of minimum degree $\deg(g(x)) = r$. Each codeword of \mathcal{C} can be expressed as a polynomial $c(x)$ in $\mathbb{F}_2[x]$ with non-zero coefficient at the positions where the i -th bit of codeword $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$ is 1. In the finite field of order two, the non-zero coefficients only equal to 1. Denoted by $\mathcal{C} = \langle g(x) \rangle$, a cyclic code \mathcal{C} generated by its *generator polynomial* $g(x)$. The set of codewords then can be written as $\mathcal{C} = \{m(x)g(x)\}$, where $m(x)$ is some message polynomial of degree $\deg(m(x)) < k$. If $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r$, then \mathcal{C} is generated by the rows of the generator matrix

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & 0 & g_0 & g_1 & \dots & g_r \end{bmatrix} = \begin{bmatrix} g(x) & & & & & & \\ & xg(x) & & & & & \\ & & \ddots & & & & \\ & & & x^{k-1}g(x) & & & \end{bmatrix}.$$

Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be two linear cyclic codes of the same length with $k_1 > k_2$. Let $c'(x)$ and $c''(x)$ be a codeword of \mathcal{C}_1 and \mathcal{C}_2 , respectively. If \mathcal{C}_1 contains \mathcal{C}_2 , $\mathcal{C}_2 \subset \mathcal{C}_1$, then the generator polynomial $g_1(x)$ divides every codeword of \mathcal{C}_2 , that is

$$\frac{x^s c''(x)}{g_1(x)} = f(x) + r(x), \quad (1)$$

where $r(x) = 0$ for every $c''(x) \in \mathcal{C}_2$, and $0 \leq s \leq k-1$ represents the s -th shifts of $c''(x)$. Then, $f(x) = \frac{g_2(x)}{g_1(x)}$ is a polynomial of degree $\deg(f(x)) = k_1 - k_2$.

The binary *dual code*, \mathcal{C}^\perp , of a binary code \mathcal{C} is defined as

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}_2^n | \forall \mathbf{u} \in \mathcal{C}, \sum_{i=1}^n u_i v_i = 0 \pmod{2}\}, \quad (2)$$

where the dimension of \mathcal{C}^\perp is equal to $n - \dim(\mathcal{C})$, that is $\dim(\mathcal{C}^\perp) + \dim(\mathcal{C}) = n$. Furthermore, denoted by $\mathcal{C}^\perp = \langle g^\perp(x) \rangle$ the dual code of \mathcal{C} and $h(x) = \frac{x^n-1}{g(x)}$ the check polynomial of \mathcal{C} , the generator polynomial $g^\perp(x)$ is given by

$$g^\perp(x) = x^{\deg(h(x))} h(x^{-1}). \quad (3)$$

If $\mathcal{C}^\perp \subseteq \mathcal{C}$, then $g(x)$ divides $g^\perp(x)$ and also every codeword of \mathcal{C}^\perp .

2) *Quadratic (Non-)Residues and Quadratic Residue Codes*: Define $\mathcal{Q}^\mathcal{R} = \{x^2 \pmod{p} | 1 \leq x \leq \frac{p-1}{2}\}$ a quadratic residue set of size $\frac{p-1}{2}$, where p is a prime. Then the corresponding quadratic non-residue set $\mathcal{Q}^{\mathcal{NR}} = \{1, 2, \dots, p-1\} \setminus \mathcal{Q}^\mathcal{R}$ of the same size is the *similar set* of $\mathcal{Q}^\mathcal{R}$. Denoted by $\bar{\mathcal{Q}}^\mathcal{R}$ and $\bar{\mathcal{Q}}^{\mathcal{NR}}$ the *complementary set* of $\mathcal{Q}^\mathcal{R}$ and $\mathcal{Q}^{\mathcal{NR}}$, respectively. That is, $\bar{\mathcal{Q}}^\mathcal{R} = \{0, \mathcal{Q}^{\mathcal{NR}}\}$ and $\bar{\mathcal{Q}}^{\mathcal{NR}} = \{0, \mathcal{Q}^\mathcal{R}\}$.

Let $Q^r(x)$ and $Q^{nr}(x)$ be the generator polynomial of two cyclic codes generate from $\mathcal{Q}^\mathcal{R}$ and $\mathcal{Q}^{\mathcal{NR}}$, respectively. Then, \mathcal{C}_R and \mathcal{C}_{NR} are quadratic residue codes over \mathbb{F}_2 with generator polynomials

$$\mathcal{C}_R = \langle Q^r(x) \rangle = \langle \prod_{r \in \mathcal{Q}^\mathcal{R}} (x - \alpha^r) \rangle \quad (4)$$

and

$$\mathcal{C}_{NR} = \langle Q^{nr}(x) \rangle = \langle \prod_{nr \in \mathcal{Q}^{\mathcal{NR}}} (x - \alpha^{nr}) \rangle, \quad (5)$$

where α is a primitive p -th root of unity in the extension field \mathbb{F}_{2^t} that containing \mathbb{F}_2 . Similarly, the quadratic residue codes constructed from the complementary sets are denoted as $\bar{\mathcal{C}}_R = \langle \bar{Q}^r(x) \rangle$ and $\bar{\mathcal{C}}_{NR} = \langle \bar{Q}^{nr}(x) \rangle$.

III. QUANTUM SYNCHRONIZABLE CODE

In this section, we briefly introduce the concept of quantum synchronizable codes and procedures of synchronization recovery for quantum information.

A. Quantum Synchronizable Coding

In very recent work [13]-[15], a general framework for constructing quantum synchronizable codes of CSS structure relying on a pair of classical cyclic codes with special property was introduced.

Theorem 1: [14] Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be two cyclic codes of parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$ with $k_1 > k_2$, respectively. Define $f(x)$ of degree $k_1 - k_2$ to be the quotient of $\frac{g_2(x)}{g_1(x)}$ over $\mathbb{F}_2[x]/(x^n - 1)$. If $\mathcal{C}_2 \subset \mathcal{C}_1$ and $\mathcal{C}_2^\perp \subseteq \mathcal{C}_2$, then for any pair of non-negative integers c_l, c_r satisfying $c_l + c_r < \text{ord}(f(x))$, there exists a $(c_l, c_r) - \llbracket n + c_l + c_r, 2k_2 - n \rrbracket$ quantum synchronizable code that corrects at least up to $\lfloor \frac{d_1-1}{2} \rfloor$ bit errors and $\lfloor \frac{d_2-1}{2} \rfloor$ phase errors. ■

The quantum synchronizable codes described in *Theorem 1* require a pair of cyclic codes $\mathcal{C}_1, \mathcal{C}_2$ of the same length, and the dimension of $k_1 > k_2 > \lceil \frac{n}{2} \rceil$. A misalignment of θ qubits can be recovered if $-c_l \leq \theta \leq c_r$, where a negative θ means that a misalignment occurs towards the left. Hence, it is a quantum synchronizable code that encodes $2k_2 - n$ logic qubits into $n + c_l + c_r$ physical qubits and be able to correct up to c_l and c_r misalignments towards the left and right, respectively. The maximal tolerance of quantum synchronization error, $-c_l \leq \theta \leq c_r$, is given by $c_l + c_r < \text{ord}(f(x))$. The order of $f(x)$, $\text{ord}(f(x))$, is the smallest integer z such that $f(x)$ divides $x^z + 1$ over \mathbb{F}_2 . To design a good quantum synchronizable codes, it is generally desirable to have a pair of cyclic codes with good distance property while $\text{ord}(f(x))$ is maximized.

B. Encoding

Since $\dim(\mathcal{C}_2) = k_2$ and $\dim(\mathcal{C}_2^\perp) = n - k_2$, then the dimension of cosets $\dim(\mathcal{C}_2/\mathcal{C}_2^\perp) = k_2 - n + k_2 = 2k_2 - n$. Hence, the size of the cosets is 2^{2k_2-n} . Let $\mathcal{B} = \{b_i(x) | 0 < i \leq 2^{2k_2-n}\}$ be the representative of the cosets, then the vector space \mathbb{Q} of dimension 2^{2k_2-n} forms an orthonormal quantum state basis with

$$|q_i(x)\rangle = |\mathcal{C}_2^\perp + b_i(x) + g_1(x)\rangle, \quad (6)$$

where $|q_i(x)\rangle \in \mathbb{Q}$, $g_1(x)$ is the generator polynomial of \mathcal{C}_1 and $b_i(x) \in \mathcal{B}$.

Using the standard encoder for CSS codes, the encoding stage described in [13] encodes the state $|\psi\rangle$ into $|\psi\rangle_{\text{enc}} = \sum_i \alpha_i |\mathbf{q}_i\rangle$ through some unitary operator, where each \mathbf{q}_i is the n -tuple binary vector representing the coefficients of each $q_i(x)$ in (6). In addition to this, extra $c_l + c_r < \text{ord}(f(x))$ ancilla qubits used to take $|\psi\rangle_{\text{enc}}$ to an $n + c_l + c_r$ -qubit state

$$|0\rangle^{\otimes c_l} |\psi\rangle_{\text{enc}} |0\rangle^{\otimes c_r} = \sum_i \alpha_i |\mathbf{l}_i, \mathbf{q}_i, \mathbf{r}_i\rangle, \quad (7)$$

where \mathbf{l}_i and \mathbf{r}_i are the last c_l and the first c_r portions of the vector \mathbf{q}_i , respectively. Hence, (7) is the final state ready to transmit.

C. Synchronization Recovery

The procedures for error correction and block synchronization are as follows. Define a window frame $\mathcal{W} = (w_{c_l}, w_{c_l+1}, \dots, w_{c_l+n-1})$, and block frame $\mathcal{T} = (t_0, t_1, \dots, t_{n+c_l+c_r-1})$ of the encoded state. A synchronization error occurs if a block of $n + c_l + c_r$ consecutive qubits misaligned by $-c_l \leq \theta \leq c_r$ qubits. Then $\mathcal{W} = (t_{c_l+\theta}, t_{c_l+1+\theta}, \dots, t_{c_l+n-1+\theta})$ for some value of θ . If $\theta = 0$, it means no misalignment occurred. The first stage of error correction is to make \mathcal{W} error free from standard bit errors by performing syndrome measurements on the corrupted encoded state, that is

$$E|\psi\rangle_{enc}|0\rangle^{\otimes n-k_1} \rightarrow E|\psi\rangle_{enc}|\mathcal{H}_{C_1}\mathbf{e}_{q_i}\rangle. \quad (8)$$

The operator E is the n -fold tensor product of linear combinations of Pauli operators, and \mathcal{H}_{C_1} the $n - k_1$ parity-check matrix (stabilizer generators) of code \mathcal{C}_1 . Finally, the result of $\mathcal{H}_{C_1}\mathbf{e}_{q_i}$ is the error syndrome of the window \mathcal{W} . If at most $\lfloor \frac{d_1-1}{2} \rfloor$ bit errors were introduced by E , these errors can be corrected to make the window \mathcal{W} error free.

The procedure of synchronization recovery performed by applying a two-stage polynomial division on the bit error free window \mathcal{W} . Since $\mathcal{C}_2^\perp \subset \mathcal{C}_2 \subset \mathcal{C}_1$, the generator polynomial $g_1(x)$ divides every $q_i(x)$ given in (6), which implies

$$c_j^\perp(x) + b_i(x) + g_1(x) = v_1(x)f(x)g_1(x) + v_2(x)f(x)g_1(x) + g_1(x), \quad (9)$$

for some polynomials $v_1(x)$ and $v_2(x)$ of degree less than k_2 . Note that a bit error free window \mathcal{W} contains a cyclic shifted coefficient vectors of the correct polynomials. If a misalignment of θ qubits occurs, define $a^\theta(x) = x^\theta(c_j^\perp(x) + b_i(x) + g_1(x))$. To extract the exact number of misaligned qubits, the two-stage polynomial division on $a^\theta(x)$ is required. Since $c_j^\perp(x) + b_i(x) + g_1(x)$ divides $g_1(x)$ and the quotient $u(x)$ divided by $f(x)$ gives remainder of $r(x) = 1$, for θ misaligned qubits, we have

$$\frac{a^\theta(x)}{g_1(x)f(x)} = u^\theta(x) + r^\theta(x), \quad (10)$$

where the remainder $r^\theta(x) = x^\theta \pmod{f(x)}$. Hence, for $-c_l \leq \theta \leq c_r$, the remainder $r^\theta(x)$ is distinct. From x^θ , we know how many qubits the original frame \mathcal{T} is misaligned and in which direction. By cyclicly shifting \mathcal{T} to recover the correct block of qubits, any additional bit errors outside the window \mathcal{W} is then corrected using \mathcal{H}_{C_1} . Finally, at most $\lfloor \frac{d_2-1}{2} \rfloor$ phase errors on the corrupted states can be corrected by applying \mathcal{H}_{C_2} in the same fashion as a standard CSS code does.

The tolerance of synchronization error for coding scheme given in [13] is improved from $c_l + c_r < k_1 - k_2$ to $c_l + c_r < \text{ord}(f(x))$ [14]. Note that $\deg(f(x)) < \text{ord}(f(x))$. In the following sections of the paper, we introduce a new method to construct quantum synchronizable codes of $\text{ord}(f(x)) = n$.

IV. AUGMENTED CYCLIC CODES

We now provide a construction method of quantum synchronizable codes designed from *quadratic residue sets*. The outcome is a pair of cyclic codes \mathcal{C}_1 and \mathcal{C}_2 with $k_1 > k_2$ that satisfy $\mathcal{C}_2^\perp \subseteq \mathcal{C}_2 \subset \mathcal{C}_1$. We first construct a cyclic code \mathcal{C}_2 using quadratic residue sets, where its dual code, \mathcal{C}_2^\perp , is a subspace of \mathcal{C}_2 . We then obtain \mathcal{C}_1 by inserting codewords into \mathcal{C}_2 . Note that \mathcal{C}_1 is also a cyclic code of higher dimension and satisfy $\mathcal{C}_2 \subset \mathcal{C}_1$.

Theorem 2: Let $\mathcal{C}_2 = \langle Q^r(x) \rangle$ and $\mathcal{C}_1 = \langle g_1(x) = \frac{Q^r(x)}{f(x)} \rangle$ be two cyclic codes of length $p = 4m - 1$ with $k_1 > k_2$, $m = 2^l$ and p is a prime. Then $\text{ord}(f(x)) = p$ and $\mathcal{C}_2^\perp = \langle \bar{Q}^r(x) \rangle$ is the dual of \mathcal{C}_2 . Moreover, there exists at least one \mathcal{C}_1 such that $\mathcal{C}_2^\perp \subset \mathcal{C}_2 \subset \mathcal{C}_1$ is satisfied. For every non-negative pair of c_l and c_r that satisfies $c_l + c_r < p$, there exists a $(c_l, c_r) - \llbracket [p + c_l + c_r, 2k_2 - p = 1] \rrbracket$ quantum synchronizable code that corrects $\lfloor \frac{d_1-1}{2} \rfloor$ bit error and $\lfloor \frac{d_2-1}{2} \rfloor$ phase error.

A. Dual-containing Cyclic Codes: $\mathcal{C}_2^\perp \subset \mathcal{C}_2$

From (4), we know that the generator polynomial of any quadratic residue codes of length p is

$$\mathcal{C}_R = \langle Q^r(x) \rangle \quad \text{and} \quad \mathcal{C}_{NR} = \langle Q^{nr}(x) \rangle. \quad (11)$$

Then the generator polynomial of cyclic codes $\bar{\mathcal{C}}_Q$ and $\bar{\mathcal{C}}_{NR}$ constructed from the complementary set $\bar{\mathcal{Q}}^R$ and $\bar{\mathcal{Q}}^{NR}$ are given by [18, P.481]

$$\bar{\mathcal{C}}_R = \langle \bar{Q}^r(x) \rangle = \langle (x-1)Q^r(x) \rangle \quad (12)$$

and

$$\bar{\mathcal{C}}_{NR} = \langle \bar{Q}^{nr}(x) \rangle = \langle (x-1)Q^{nr}(x) \rangle. \quad (13)$$

Lemma 1: For a prime $p = 4m - 1$, the associated quadratic residue codes \mathcal{C}_R , \mathcal{C}_{NR} , $\bar{\mathcal{C}}_R$ and $\bar{\mathcal{C}}_{NR}$ are cyclic codes of code length p and

$$1) \quad \mathcal{C}_R^\perp = \bar{\mathcal{C}}_R, \quad \mathcal{C}_{NR}^\perp = \bar{\mathcal{C}}_{NR}. \quad (14)$$

$$2) \quad \mathcal{C}_R^\perp \subset \mathcal{C}_R, \quad \mathcal{C}_{NR}^\perp \subset \mathcal{C}_{NR}. \quad (15)$$

■

Proof: We know that if α is a primitive p -th root of unity in a field, then the ring $\mathbb{F}_2[x]/(x^p - 1)$ is equal to

$$x^p - 1 = (x-1)Q^r(x)Q^{nr}(x), \quad (16)$$

where $Q^r(x) = \prod_{r \in \mathcal{Q}^R} (x - \alpha^r)$ and $Q^{nr}(x) = \prod_{r \in \mathcal{Q}^{NR}} (x - \alpha^{nr})$. The zeros of $Q^r(x)$ and $Q^{nr}(x)$ are $\{\alpha^r | r \in \mathcal{Q}^R\}$ and $\{\alpha^{nr} | nr \in \mathcal{Q}^{NR}\}$, respectively. Hence by (3), the zeros of \mathcal{C}_R^\perp are 1 and α^{-r} , and the zeros of \mathcal{C}_{NR}^\perp are 1 and α^{-nr} . Moreover, since $\alpha^e \in \mathcal{Q}^R$ iff e is even, and $\alpha^e \in \mathcal{Q}^{NR}$ iff e is odd, then $-r \in \mathcal{Q}^{NR}$ and $-nr \in \mathcal{Q}^R$. Hence, $\mathcal{C}_R^\perp = \bar{\mathcal{C}}_R$ and $\mathcal{C}_{NR}^\perp = \bar{\mathcal{C}}_{NR}$.

Furthermore, we know that \mathcal{Q}^R and \mathcal{Q}^{NR} are disjoint sets of size $\frac{p-1}{2}$, then $\deg(Q^r(x)) = \deg(Q^{nr}(x)) = \frac{p-1}{2}$. From (12) we know that $\deg(\bar{Q}^r(x)) = \frac{p-1}{2} + 1$ which implies $\deg(Q^r(x)) + \deg(\bar{Q}^r(x)) = p$, and $Q^r(x)$ divides $\bar{Q}^r(x)$. Hence $\mathcal{C}_R^\perp \subset \mathcal{C}_R$, and for the codes \mathcal{C}_{NR} and $\bar{\mathcal{C}}_{NR}$, similar result is obtained, that is $\mathcal{C}_{NR}^\perp \subset \mathcal{C}_{NR}$.

We have now completed the proof. \blacksquare

Example 1: Consider the quadratic residue set

$$\mathcal{Q}^{\mathcal{R}} = \{1, 2^2, 3^2, 4^2, \dots, 15^2\} \pmod{31} \\ = \{1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8\}. \quad (17)$$

The quadratic residue codes \mathcal{C}_R and $\bar{\mathcal{C}}_R$ of length $p = 31$ have generator polynomial

$$Q^r(x) = x^{15} + x^{12} + x^7 + x^6 + x^2 + x + 1$$

and

$$\bar{Q}^r(x) = x^{16} + x^{13} + x^{10} + x^8 + x^4 + x^3 + x + 1.$$

They are obtained from $\mathcal{Q}^{\mathcal{R}}$ and $\bar{\mathcal{Q}}^{\mathcal{R}}$, respectively. Since $\text{lcm}(Q^r(x), \bar{Q}^r(x)) = x^{31} + 1$, from Lemma 1 and Equation (3), we know that $\bar{Q}^r(x)$ is the generator polynomial of the dual-code \mathcal{C}_R^\perp . Furthermore, because $Q^r(x)$ divides $\bar{Q}^r(x)$ and $\dim(\mathcal{C}_R) + \dim(\bar{\mathcal{C}}_R) = p$, then $\bar{\mathcal{C}}_R = \mathcal{C}_R^\perp \subset \mathcal{C}_R$. \square

Corollary 1: Let $\mathcal{C}_2 = \mathcal{C}_R$ be a cyclic code of length p and $\dim(\mathcal{C}_2) = \frac{p+1}{2}$, then $\mathcal{C}_2^\perp = \bar{\mathcal{C}}_R$ is the dual code of \mathcal{C}_2 with dimension $\dim(\mathcal{C}_2) = \frac{p-1}{2}$ that generates a sub-code of \mathcal{C}_2 . Hence, $\mathcal{C}_2 \supset \mathcal{C}_2^\perp$ is a dual-containing cyclic code. \blacksquare

B. Augmentation of \mathcal{C}_2

To obtain another cyclic code \mathcal{C}_1 such that $\mathcal{C}_2 \subset \mathcal{C}_1$, we increase the number of codewords to the pre-obtained cyclic code \mathcal{C}_2 , the resulting cyclic code \mathcal{C}_1 is called *augmented cyclic code*. Let $\mathcal{C}_2 = \langle g_2(x) \rangle$ and $\mathcal{C}_1 = \langle g_1(x) \rangle$, if $\mathcal{C}_2 \subset \mathcal{C}_1$, $\deg(g_1(x)) < \deg(g_2(x))$. This is equivalent to increase the dimension of \mathcal{C}_2 . Hence, $g_2(x)$ is a *reducible* monic polynomial of degree $\frac{p-1}{2}$.

Proposition 1: Given $\mathcal{C}_2 = \mathcal{C}_R$ is a cyclic code of length p constructed from quadratic residue set with polynomial $g_2(x) = \prod_{r \in \mathcal{Q}^{\mathcal{R}}} (x - \alpha^r)$, if $m = 2^l, l \in \mathbb{Z}$ and $p = 4m - 1$ is a prime, then

$$g_2(x) = \prod_j F_j(x), \quad (18)$$

where each $F_j(x)$ is an irreducible minimal polynomial over \mathbb{F}_q of degree $l + 2$. Denoted by $\mathcal{F} = \{F_j(x) | 1 \leq j \leq k'\}$ a set of irreducible minimal polynomial, then $|\mathcal{F}| = \frac{2^{l+1}-1}{l+2}$. \blacksquare

To analyse Proposition 1, we need the following definition of *cyclotomic cosets*.

Definition 1: The *cyclotomic cosets* of elements of field \mathbb{F}_{q^t} containing integer i is defined as

$$S_i = \{iq^s | 0 \leq s \leq t' - 1\} \pmod{q^t - 1} \quad (19)$$

where t' is the smallest positive integer such that $iq^{t'} = i \pmod{q^t - 1}$. If $i \in S_i$ is the smallest integer, then i is the coset representatives of S_i . \square

For arbitrary prime $p = 4m - 1$, denoted by $T = \{i | i \in \mathbb{Z}\}$ the set of coset representatives of \mathbb{F}_{q^t} , then a $\mathcal{Q}^{\mathcal{R}}$ set of size $\frac{p-1}{2}$ is a union of some number of cyclotomic cosets of \mathbb{F}_{q^t} . We state the following lemma.

Lemma 2: For $m = 2^l, l \in \mathbb{Z}$, and $p = 4m - 1$ is a prime, the quadratic residue set $\mathcal{Q}^{\mathcal{R}}$ of size $\frac{p-1}{2}$ is a union

$$\mathcal{Q}^{\mathcal{R}} = \bigcup_{\{i \in \mathcal{Q}^{\mathcal{R}} | i \in T\}} S_i, \quad (20)$$

where each cyclotomic coset is of size $|S_i| = l + 2$. \blacksquare

Proof: If $m = 2^l, p = 2^{l+2} - 1$ and $|\mathcal{Q}^{\mathcal{R}}| = 2^{l+1} - 1$. By the property of Mersenne number, if p is a prime, $l + 2$ is a prime which implies that $l + 1$ is not a prime. Hence, $\mathcal{Q}^{\mathcal{R}}$ is a union of disjoint cosets. Furthermore, let $t = l + 2$, by definition 1, $iq^{t'} = i \pmod{2^t - 1}$ when $t' = t$, thus, each cosets S_i is closed under multiplication of 2. Therefore, each $|S_i| = t = l + 2$ and $\mathcal{Q}^{\mathcal{R}}$ is a union of $\frac{2^{l+1}-1}{l+2}$ cyclotomic cosets of \mathbb{F}_{q^t} . \blacksquare

Corollary 2: The minimal polynomial $F_i(x)$ of an element $\alpha^i \in \mathbb{F}_{q^t}$ is given by

$$F_i(x) = \prod_{s=0}^{t-1} (x - \alpha^{iq^s}) \quad (21)$$

with $\deg(F_i(x)) = t$, and α is a primitive element of \mathbb{F}_{q^t} . \blacksquare

It is obvious that every element of the same coset S_i has the same minimal polynomial over \mathbb{F}_q because $F_i(\alpha^{iq^0}) = F_i(\alpha^{iq^1}) = \dots F_i(\alpha^{iq^{(t-1)}}) = 0 \pmod{q}$. Furthermore, each $F_i(x)$ is irreducible and monic since S_i does not contain any smaller nonzero subset and

$$F_i(0) \neq 0.$$

Based on Equation (18), we obtain the generator polynomial $g_1(x)$ for \mathcal{C}_1 by removing arbitrary one or multiple minimal polynomials from $g_2(x)$. Let $\mathcal{F} = \{F_i(x) | i \in \mathcal{Q}^{\mathcal{R}}\}$, $T^r = \{i | i \in \mathcal{Q}^{\mathcal{R}}\}$ and $v = |\mathcal{F}| = \frac{2^{l+1}-1}{l+2}$. If $f(x) = \frac{g_2(x)}{g_1(x)}$, we have

$$f(x) = \prod_{1 \leq j \leq \binom{v}{z}, z: 1 \leq z < v-1} F_{\{\pi^z\{T^r\}\}_j}(x), \quad (22)$$

where

$$\pi^z\{T^r\} = \binom{v}{z} \quad (23)$$

is the total number of combinations to remove z minimal polynomials from \mathcal{F} . Let $\{\pi^z\{T^r\}\}_j$ denote the j -th combination of such operation. Hence, the total number of different $g_1(x)$ we can get is then equal to

$$\sum_{z=1}^{v-1} \binom{v}{z}. \quad (24)$$

The dimension of \mathcal{C}_1 is then determined by

$$\dim(\mathcal{C}_1) = p - \deg\left(\frac{g_2(x)}{f(x)}\right) \\ = p - \deg(g_2(x)) + z(l + 2). \quad (25)$$

Thus, the resulting \mathcal{C}_1 is a cyclic code of the same length as \mathcal{C}_2 with $\dim(\mathcal{C}_1) > \dim(\mathcal{C}_2)$, and we have $\mathcal{C}_2 \subset \mathcal{C}_1$.

C. Maximum misalignment tolerance

In the context of quantum synchronizable codes, we like to maximize the tolerance of misalignment error by maximizing $\text{ord}(f(x))$. It is known that the maximum misalignment error that is tolerable by a quantum synchronizable code is upper bounded by its code length p [14]. To achieve the upper bound, that is $\text{ord}(f(x)) = p$, $\gcd(f(x), g_2(x)) = x^p - 1$.

Theorem 3: [17, P.89] A polynomial $f(x) \in \mathbb{F}_q$ of degree m is a primitive polynomial over \mathbb{F}_q iff $f(x)$ is monic, that is $f(0) \neq 0$ and $\text{ord}(f(x)) = q^m - 1$. ■

Based on *Theorem 3*, we have the following result show that the proposed quantum synchronizable codes have maximum tolerance of misalignment error.

Corollary 3: For $m = 2^l$ and $p = 4m - 1$ is a prime, if $\mathcal{C}_2 = \langle g_2(x) \rangle$, $\mathcal{C}_1 = \langle g_1(x) \rangle$ such that $g_2(x) = g_1(x)f(x)$, then each $F_i(x)$ is a primitive polynomial of degree $l + 2$ and $\text{ord}(f(x)) = 2^{l+2} - 1$. ■

By Equations (16) and (18), we know that $x^p - 1 = x^{2^{l+2}-1} - 1$ is divisible by every $F_i(x)$. Since $\deg(F_i(x)) = l + 2$, we have $\text{ord}(F_i(x)) = 2^{\deg(F_i(x))} - 1 = 2^{l+2} - 1 = p$. Thus, by *Theorem 3*, every $F_i(x)$ is a primitive polynomial that has order equal to the code length p . Moreover, if $F_i(x)$ and $F_{i'}(x)$, $i \neq i'$, are two difference primitive polynomials, then $\text{lcm}(F_i(x), F_{i'}(x)) = x^p - 1$. Hence, for arbitrary number of $F_i(x)$ removed from $g_2(x)$, the order of $f(x)$ is always equal to the code length p .

Example 2: Continue with *Example 1*. When $l = 3$, $p = 2^{l+2} - 1$ is a prime integer such that the quadratic residue set $\mathcal{Q}^R = \{x^2 \pmod{p} \mid 1 \leq x \leq 2^{l+1} - 1\}$ is equivalent to the union of $\frac{2^4-1}{5} = 3$ cyclotomic cosets of field \mathbb{F}_{2^5} , that is

$$\mathcal{Q}^R = S_1 \cup S_5 \cup S_7,$$

where

$$\begin{aligned} S_1 &= \{1, 2, 4, 8, 16\}, \\ S_5 &= \{5, 10, 20, 9, 18\}, \\ S_7 &= \{7, 14, 28, 25, 19\}. \end{aligned} \quad (26)$$

Let $\mathcal{C}_2 = \langle Q^r(x) \rangle$, then

$$Q^r(x) = F_1(x)F_5(x)F_7(x),$$

where

$$\begin{aligned} F_1(x) &= x^5 + x^2 + 1, \\ F_5(x) &= x^5 + x^4 + x^2 + x + 1, \\ F_7(x) &= x^5 + x^3 + x^2 + x + 1 \end{aligned}$$

are irreducible minimal polynomials over \mathbb{F}_2 for elements α , α^5 and α^7 in \mathbb{F}_{2^5} . Furthermore, since each one of $F_1(x)$, $F_5(x)$ and $F_7(x)$ divides $x^{31} - 1$, let $\mathcal{C}_1 = \langle g_1(x) = \frac{Q^r(x)}{f(x)} \rangle$, if $z = 1$, $f(x) = F_j(x)$, $j \in \{1, 5, 7\}$, the dimension of \mathcal{C}_1 is equal to $\dim(\mathcal{C}_1) = p - \deg(g_2(x)) + z(l + 2) = 31 - 15 + 5 = 21$. Alternatively, if $z = 2$, then $f(x) = F_{j_1}(x)F_{j_2}(x)$ and $j_1, j_2 \in \{1, 5, 7\}$ for $j_1 \neq j_2$, the dimension of \mathcal{C}_1 is $\dim(g_1(x)) = 31 - 15 + 10 = 26$. In both cases, the $\text{ord}(f(x)) = 2^{l+2} - 1 = p$.

Since $\deg(Q^r(x)) = 15$, $\dim(\mathcal{C}_2) = 16$, thus, for arbitrary pair of non-negative integer c_l and c_r such that $c_l + c_r < 31$, we have a $(c_l, c_r) - [[p + c_l + c_r, 1]]$ quantum synchronizable code. If $c_l + c_r = 30$, the corresponding quantum synchronizable code $(c_l, c_r) - [[61, 1]]$ is capable to recover up to the maximum number of misalignment error it tolerates. □

V. CONCLUSION

We studied the importance of block synchronization in quantum communication and quantum computations. We then proposed a method to construct quantum synchronizable codes by designing augmented cyclic codes from another cyclic code. The proposed method based on the notion of quadratic residue sets. We showed the tolerance of synchronization error meet the upper bound under certain condition.

For future work, one will generalize the construction to any quadratic residue set over non-binary field \mathbb{F}_{q^t} . Secondly, note that the proposed quantum synchronizable codes only encode $k = 1$ logical qubit into $p + c_l + c_r$ physical qubits due to the fact that $\dim(\mathcal{C}_2) = \frac{p+1}{2}$, therefore, design of quantum synchronizable codes from quadratic residue sets with variable dimensions is desirable. Lastly, the distance d_1 and d_2 should also be maximized for a given n .

REFERENCES

- [1] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 52, pp. 2493-2496, 1995.
- [2] E. Knill, R. Laflamme, and L. Viola, "Theory of Quantum Error Correction for General Noise", *Phys. Rev. Lett.*, vol. 84, pp. 2525-2528, 2000.
- [3] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", *Cambridge Uni. Press*, New York, 2000.
- [4] A. M. Steane, "Error Correcting Codes in Quantum Theory," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.
- [5] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098-1105, 1996.
- [6] A. Steane, "Multiple particle interference and quantum error correction," *Proc. Royal Soci. of London*, vol. 452, no. 1954, pp. 2551-2577, 1996.
- [7] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900-911, 1997.
- [8] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862-1868, 1996.
- [9] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Infor. Theory*, vol. 50, pp. 2315-2330, 2004.
- [10] T. Brun, I. Devetak and M. H. Hsieh, "Correcting Quantum Errors with Entanglement", *arXiv preprint quant-ph/0610092*, 2006.
- [11] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, "Spatially coupled quasi-cyclic quantum LDPC codes," in *IEEE Proc. Int. Symp. Infor. Theory*, pp. 638-642, 2011.
- [12] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum Error Correction beyond the Bounded Distance Decoding Limit," *IEEE Trans. Infor. Theory*, vol. 58, no. 2, pp. 1223-1230, 2012.
- [13] Y. Fujiwara, "Block Synchronization for Quantum Information", *Phys. Rev. A*, vol. 87, 022344, 2013.
- [14] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, "Algebraic techniques in designing quantum synchronizable codes", *Phy. Rev. A*, vol. 88, 012318, 2013.
- [15] Y. Fujiwara and P. Vandendriessche, "Quantum Synchronizable Codes From Finite Geometries", *arxiv.org/abs/1311.3416*
- [16] J. L. Massey, "Reversible Codes", *Inform. and Control*, vol. 7, pp. 369-380, 1964.
- [17] R. Lidl and H. Niederreiter, "Finite Fields", 2nd edition, *Cambridge Uni. Press*, Cambridge, 1997.
- [18] F. J. MacWilliams and N. J. A. Sloane, "The theory of error-correcting codes", North-holland Publishing Comp. 2nd edition, 1978.